ГЛАВА ЧЕТЫРНАДЦАТАЯ

ГРУППЫ

§. 63. Определение и примеры групп

Кольца и поля, игравшие столь большую роль в предшествующих главах, являются алгебраическими системами с двумя независимыми операциями: сложением и умножением. В различных отделах математики и в ее приложениях весьма часто встречаются, однако, и такие алгебраические системы, в которых определена лишь одна алгебраическая операция. Так, ограничиваясь пока примерами, уже появлявшимися в нашей книге, отметим, что в множестве подстановок n-й степени (см. § 3) нами была определена лишь одна операция — умножение. С другой стороны, в определение векторного пространства (§ 8) входит сложение векторов, в то время как умножение векторов не было нами определено (заметим, что умножение вектора на число не удовлетворяет данному в § 44 определению алгебраической операции).

Важнейшим типом алгебраических систем с одной операцией являются группы. Это понятие обладает чрезвычайно широкой областью применений и служит предметом большой самостоятельной науки — теории групп. Настоящая глава может рассматриваться как введение в теорию групп — в ней будут изложены элементарные сведения о группах, знакомство с которыми необходимо каждому математику; закончится глава одной менее элементарной теоремой.

Условимся, как это принято в общей теории групп, называть рассматриваемую алгебраическую операцию *умножением* и употреблять соответствующую символику. Напомним (см. § 44), что алгебраическая операция предполагается всегда выполнимой и однозначной — для любых двух элементов a и b рассматриваемого множества произведение ab существует и является однозначно определенным элементом этого множества.

Группой называется множество G с одной алгебраической операцией, ассоциативной (хотя не обязательно коммутативной), причем для этой операции должна существовать обратная операция.

При этом, ввиду возможной некоммутативности групповой операции, выполнимость обратной операции означает следующее: для любых двух элементов a и b из G существуют в G такой одно-

значно определенный элемент x и такой однозначно определенный элемент y, что

$$ax = b, \quad ya = b.$$

Если группа G состоит из конечного числа элементов, то она называется *конечной группой*, а число элементов в ней — *порядком* группы. Если операция, определенная в группе G, коммутативна, то G называется *коммутативной* или *абелевой* группой.

Укажем простейшие следствия из определения группы. На основании рассуждений, уже проводившихся в § 44, можно утверждать, что закон ассоциативности позволяет говорить однозначным образом *о произведении любого конечного числа элементов группы*, заданных (ввиду возможной некоммутативности групповой операции) в определенном порядке.

Переходим к следствиям из существования обратной операции.

Пусть в группе G дан произвольный элемент a. Из определения группы вытекает существование в G такого однозначно определенного элемента e_a, что $ae_a = a$; этот элемент играет, следовательно, роль единицы при умножении на него элемента a справа. Если b — любой другой элемент группы G и если y есть элемент группы, удовлетворяющий равенству $ya = b$, — его существование следует из определения группы, — то мы получим:

$$b = ya = y(ae_a) = (ya)e_a = be_a.$$

Таким образом, элемент e_a играет роль правой единицы по отношению ко всем элементам группы G, а не только по отношению к исходному элементу a; поэтому мы его обозначим через e'. Из однозначности, входящей в определение обратной операции, вытекает единственность этого элемента.

Таким же путем можно доказать существование и единственность в группе G элемента e'', удовлетворяющего условию $e''a = a$ для всех a из G. На самом деле элементы e' и e'' совпадают, так как из равенств $e''e' = e''$ и $e''e' = e'$ вытекает $e'' = e'$. Этим доказано, что *во всякой группе G существует однозначно определенный элемент e, удовлетворяющий условию*

$$ae = ea = a$$

для всех a из G. Этот элемент называется *единицей* группы G и обычно обозначается символом 1.

Из определения группы вытекает, далее, существование и единственность для данного элемента a таких элементов a' и a'', что

$$aa' = 1, \quad a''a = 1.$$

В действительности элементы a' и a'' совпадают: из равенств

$$a''aa' = a''(aa') = a'' \cdot 1 = a'',$$
$$a''aa' = (a''a)a' = 1 \cdot a' = a'$$

следует $a''=a'$. Этот элемент называется *обратным* элементу a и обозначается a^{-1}, т. е.

$$aa^{-1}=a^{-1}a=1.$$

Таким образом, *всякий элемент группы обладает однозначно определенным обратным элементом.*

Из последних равенств вытекает, что обратным элементом для элемента a^{-1} служит сам элемент a. Легко видеть, далее, что обратным для произведения нескольких элементов будет произведение элементов, обратных сомножителям и притом взятых в обратном порядке:

$$(a_1a_2\ldots a_{n-1}a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\ldots a_2^{-1}a_1^{-1}.$$

Наконец, обратным элементом для единицы будет сама единица.

Проверка того, является ли группой данное множество с одной операцией, весьма облегчается тем, что в определении группы требование выполнимости обратной операции можно заменить предположением о существовании единицы и обратных элементов, причем лишь с одной стороны (например, правой) и без предположения об их единственности. Это вытекает из следующей теоремы:

Множество G с одной ассоциативной операцией будет группой, если в G существует хотя бы один элемент e, обладающий свойством

$$ae=a \quad \textit{для всех } a \textit{ из } G,$$

и если среди этих правых единичных элементов существует хотя бы один такой элемент e_0, что по отношению к нему всякий элемент a из G обладает хотя бы одним правым обратным элементом a^{-1}:

$$aa^{-1}=e_0.$$

Доказательство. Пусть a^{-1} — один из правых обратных элементов для a. Тогда

$$aa^{-1}=e_0=e_0e_0=e_0aa^{-1},$$

т. е. $aa^{-1}=e_0aa^{-1}$. Умножая обе части этого равенства справа на один из элементов, правых обратных для a^{-1}, мы получим $ae_0=e_0ae_0$, откуда $a=e_0a$, так как e_0 — правая единица для G. Таким образом, элемент e_0 оказывается и левой единицей для G. Если теперь e_1 есть произвольная правая единица, e_2 — произвольная левая единица, то из равенств

$$e_2e_1=e_1 \quad \text{и} \quad e_2e_1=e_2$$

следует $e_1=e_2$, т. е. любая правая единица равна любой левой. Этим доказаны существование и единственность в множестве G единичного элемента, который обозначим, как выше, через 1.

Далее,

$$a^{-1}=a^{-1}\cdot 1=a^{-1}aa^{-1}.$$

т. е. $a^{-1}=a^{-1}aa^{-1}$, где a^{-1} есть один из правых обратных элементов для a. Умножая обе части последнего равенства справа на один из правых обратных элементов для a^{-1}, мы получаем $1=a^{-1}a$, т. е. элемент a^{-1} будет служить и левым обратным элементом для a. Если теперь a_1^{-1} — произвольный правый обратный для a, a_2^{-1} — произвольный левый обратный, то из равенств

$$a_2^{-1}aa_1^{-1}=\left(a_2^{-1}a\right)a_1^{-1}=a_1^{-1},$$

$$a_2^{-1}aa_1^{-1}=a_2^{-1}\left(aa_1^{-1}\right)=a_2^{-1}$$

следует $a_1^{-1}=a_2^{-1}$, т. е. следуют существование и единственность для всякого элемента a из G обратного элемента a^{-1}.

Теперь легко показать, что множество G будет группой. Действительно, уравнениям $ax=b$, $ya=b$ будут, как легко видеть, удовлетворять элементы

$$x=a^{-1}b, \quad y=ba^{-1}.$$

Единственность этих решений следует из того, что если, например, $ax_1=ax_2$, то, умножая обе части этого равенства слева на a^{-1}, мы получаем $x_1=x_2$. Теорема доказана.

Мы уже несколько раз встречались с понятием изоморфизма — для колец, для линейных пространств, для евклидовых пространств. Это понятие может быть определено и для групп и играет в теории групп столь же большую роль, как и в теории колец. Группы G и G' называются *изоморфными*, если между ними можно установить такое взаимно однозначное соответствие, при котором для любых элементов a, b из G и соответствующих им элементов a', b' из G' произведению ab соответствует произведение $a'b'$. Как в § 46 (для нуля и противоположного элемента в кольце), можно показать, что при изоморфном соответствии между группами G и G' единице группы G соответствует единица группы G', и если элементу a из G соответствует элемент a' из G', то элементу a^{-1} соответствует элемент a'^{-1}.

Переходя к примерам групп, отметим, что если бы операция в группе G была названа *сложением*, то единица группы называлась бы *нулем* и обозначалась символом 0, а вместо обратного элемента мы говорили бы о *противоположном элементе* и обозначали бы его через $-a$.

В качестве первого примера групп укажем, что *по сложению всякое кольцо* (*и, в частности, поле*) *является группой, притом абелевой*; это — так называемая *аддитивная группа кольца*. Это замечание сразу дает большое количество конкретных примеров групп и среди них — аддитивную группу целых чисел, аддитивную группу четных чисел, аддитивные группы рациональных чисел, действительных чисел, комплексных чисел и т. д. Заметим, что *аддитивные группы целых чисел и четных чисел изоморфны между*

собой, хотя вторая является лишь частью первой: отображение, ставящее в соответствие всякому целому числу k четное число $2k$, будет взаимно однозначным и, как легко проверить, даже изоморфным отображением первой из названных групп на вторую.

По умножению никакое кольцо не является группой, так как обратная операция — деление — не всегда выполнима. Положение не изменяется и при переходе от произвольного кольца к полю, так как в поле остается невыполнимым деление на нуль. Рассмотрим, однако, совокупность всех отличных от нуля элементов поля. Так как поле не содержит делителей нуля, т. е. произведение двух элементов, отличных от нуля, само отлично от нуля, то умножение будет для рассматриваемой совокупности алгебраической операцией, притом ассоциативной и коммутативной, причем деление уже всегда выполнимо и не выводит за пределы этой совокупности. Таким образом, *совокупность отличных от нуля элементов любого поля является абелевой группой*; эта группа называется *мультипликативной группой поля*. Примерами, сюда относящимися, будут мультипликативные группы рациональных чисел, действительных чисел, комплексных чисел.

Группу по умножению составляют, очевидно, все положительные действительные числа. *Эта группа изоморфна аддитивной группе всех действительных чисел*: ставя в соответствие всякому положительному числу a действительное число $\ln a$, мы получим взаимно однозначное отображение первой группы на вторую, которое будет изоморфизмом ввиду равенства

$$\ln(ab) = \ln a + \ln b.$$

Возьмем, далее, в поле комплексных чисел совокупность корней n-й степени из единицы. В § 19 было доказано, что произведение двух корней n-й степени из единицы, а также число, обратное к корню n-й степени из единицы, сами принадлежат к рассматриваемой совокупности чисел. Так как единица также принадлежит, понятно, к этой совокупности и так как умножение любых комплексных чисел ассоциативно и коммутативно, то мы получаем, что *корни n-й степени из единицы составляют по умножению абелеву группу, притом конечную порядка n*. Таким образом, *для любого натурального числа n существуют конечные группы порядка n*.

Группа (по умножению) корней n-й степени из единицы изоморфна аддитивной группе кольца Z_n, построенного в § 45. Действительно, если ε — первообразный корень n-й степени из единицы, то все элементы первой из названных групп имеют вид ε^k, $k=0, 1, \ldots, n-1$. Если мы поставим в соответствие всякому числу ε^k элемент C_k кольца Z_n, т. е. класс целых чисел, дающих при делении на n остаток k, то получим изоморфное соответствие между рассматриваемыми группами: если $0 \leqslant k \leqslant n-1$, $0 \leqslant l \leqslant n-1$ и если $k+l=nq+r$, где $0 \leqslant r \leqslant n-1$, а q равно 0 или 1, то $\varepsilon^k \cdot \varepsilon^l = \varepsilon^r$ и, вместе с тем, $C_k + C_l = C_r$.

Сейчас уместно указать некоторые примеры числовых множеств, не являющихся группами. Так, множество всех целых чисел не будет группой по умножению, множество всех положительных действительных чисел не будет группой по сложению, множество всех нечетных чисел не будет группой по сложению, множество всех отрицательных действительных чисел не будет группой по умножению. Проверка всех этих утверждений не представляет затруднений.

Все рассмотренные выше числовые группы являются, конечно, абелевыми. Примерами абелевых групп, составленных не из чисел, служат линейные пространства: как вытекает из их определения (см. §§ 29, 47), *всякое линейное пространство над произвольным полем P будет абелевой группой относительно операции сложения.*

Переходим к примерам некоммутативных групп.

Множество всех матриц n-го порядка над полем P не будет группой по отношению к операции умножения, так как нарушается требование о существовании обратного элемента. Если мы ограничимся, однако, лишь невырожденными матрицами, то получим уже группу. Действительно, произведение двух невырожденных матриц будет, как мы знаем, невырожденным, единичная матрица является невырожденной, всякая невырожденная матрица обладает обратной матрицей, также невырожденной, и, наконец, закон ассоциативности, выполняясь для всех матриц, справедлив, в частности, для матриц невырожденных. Можно говорить, следовательно, о *группе невырожденных матриц n-го порядка* над полем P с умножением матриц в качестве групповой операции; эта группа некоммутативна при $n \geqslant 2$.

К весьма важным примерам конечных некоммутативных групп приводит введенное в § 3 умножение подстановок. Мы знаем, что в множестве всех подстановок n-й степени умножение будет алгебраической операцией, притом ассоциативной, хотя при $n \geqslant 3$ некоммутативной, что тождественная подстановка E служит единицей этого умножения и что для всякой подстановки существует обратная подстановка. Таким образом, *множество подстановок n-й степени составляет по умножению группу, притом конечную порядка $n!$.* Эта группа называется *симметрической группой n-й степени*; она некоммутативна при $n \geqslant 3$.

Рассмотрим теперь вместо совокупности всех подстановок n-й степени лишь совокупность четных подстановок, состоящую, как мы знаем, из $\frac{1}{2}n!$ элементов. Используя доказанную в § 3 теорему о том, что четность подстановки совпадает с четностью числа транспозиций, входящих в какое-либо разложение этой подстановки в произведение транспозиций, мы получаем, что *произведение двух четных подстановок само четно*; в самом деле, представление AB в виде произведения транспозиций мы получим, записав соответствующие разложения для A и B одно за другим. Далее, ассоциативность

умножения подстановок нам известна, четность тождественной подстановки очевидна. Наконец, четность подстановки A^{-1} при четной подстановке A следует хотя бы из того, что записи этих подстановок можно получить одну из другой переменой мест верхней и нижней строк, т. е. они содержат равное число инверсий. Таким образом, *множество четных подстановок n-й степени будет по умножению конечной группой порядка* $\frac{1}{2}n!$. Эта группа называется *знакопеременной группой n-й степени*; легко проверить, что она некоммутативна при $n \geqslant 4$, хотя будет коммутативной при $n=3$.

Симметрические и знакопеременные группы играют очень большую роль в теории конечных групп, а также в теории Галуа. Заметим, что было бы невозможно, по аналогии со знакопеременными группами, построить группу по умножению из нечетных подстановок, так как произведение двух нечетных подстановок всегда есть четная подстановка.

Большое число разнообразных примеров групп доставляют различные ветви геометрии. Укажем один простейший пример такого рода: множество всех вращений шара около его центра будет группой, притом некоммутативной, если произведением двух вращений мы назовем результат их последовательного выполнения.

§ 64. Подгруппы

Подмножество A группы G называется *подгруппой* этой группы, если оно само является группой относительно операции, определенной в группе G.

При проверке того, является ли подмножество A группы G подгруппой этой группы, достаточно проверить: 1) содержится ли в A произведение любых двух элементов из A; 2) содержит ли A вместе со всяким своим элементом и его обратный элемент. Действительно, из справедливости закона ассоциативности в группе G следует его справедливость для элементов из A, а принадлежность к A единицы группы G вытекает из 2) и 1).

Многие из групп, указанных в предшествующем параграфе, являются подгруппами других групп, также там указанных. Так, аддитивная группа четных чисел является подгруппой аддитивной группы всех целых чисел, а последняя в свою очередь есть подгруппа аддитивной группы рациональных чисел. Все эти группы, как и вообще аддитивные группы чисел, являются подгруппами аддитивной группы комплексных чисел. Мультипликативная группа положительных действительных чисел является подгруппой мультипликативной группы всех отличных от нуля действительных чисел. Знакопеременная группа n-й степени есть подгруппа симметрической группы этой же степени.